Vind ik dit leuk? Een fundamenteel privacyperspectief op monitoring en profilingtechnologieën

C Roosendaal, A.P.

Published in:
Privacy en informatie

Publication date:
2011

Document Version
Publisher's PDF, also known as Version of record

Mr. A. Roosendaal MPhil[*]

Vind ik dit leuk?

Een fundamenteel privacyperspectief op monitoring en profilingtechnologieën

94

Trefwoorden:
contextueleintegriteit,informationelezelfbeschikking, cookies, digitale vergetelheid

Het gebruik van cookies voor het monitoren van webgedrag ten behoeve van targeted advertising is een veelbesproken onderwerp. Daarbij komt vaak de mogelijke strijd met gegevensbescherming aan de orde maar blijven meer fundamentelenoties over het belang van privacy ten onrechte onderbelicht.Het gaat daarbij om het beschermen van de individuele autonomie, het kunnen maken van vrije keuzes en vrij bepalen van doelen. Deze bijdrage beoogt het verband tussen privacy, autonomie, identiteit en gegevensbescherming uiteen te zetten en belicht vervolgens hoe de technologie deze concepten beïnvloedt. Aan de hand van een concrete casus, de 'Vind ik leuk'-knop van Facebook, wordt duidelijk dat privacy en autonomie wel degelijk in het geding zijn. Afsluitend wordt een alternatieve denkrichting voor gegevensbescherming gegeven met referentie aan recente ontwikkelingen bij de Amerikaanse Federal Trade Commission. Als belangrijkste aandachtspunten gelden het verdwijnende belang van het onderscheid tussen persoonsgegevens en andere gegevens en de praktijk van grote gegevenssets in plaats van losse gegevens.

1 Inleiding

Het gebruik van cookies om surfgedrag van internetgebruikers te monitoren is op zich niets nieuws.[1] Het wettelijk kader is echter sterk in beweging. In Nederland wordt hard gewerkt aan de implementatie van nieuwe regelgevingbetreffendecookies zoals deze is voorgeschreven in Richtlijn 2009/136/EG[2] van het Europees Parlement en die eind mei in alle EU-lidstaten moet zijn ingevoerd. De Richtlijn gaat ervan uit dat cookies gebruikt worden om persoonsgegevens te verzamelen aangezien er sterk gekeken is naar de wijze van toestemming geven voor die gegevensverwerking als bepaald in de algemene Dataprotectierichtlijn (Richtlijn 95/46/EG).[3] Al eerder werd in dit tijdschrift aandacht besteed aan de nieuwe regels voor cookies en het vereiste van toestemming.[4] Zuiderveen Borgesius concludeerde dat toestemming door middel van browserinstellingen waarschijnlijk niet voldoet aan de vereisten voor toestemming, een stelling die ik volledig onderschrijf. In zijn privacyperspectief op het gebruik van cookies voor behavioural targeting[5] stelde Van der Sloot dat cookiegebruik voor behavioural targeting geen inherent privacyprobleem oplevert. Het is volgens hem meer een probleem voor gegevensbescherming waar vervolgens wel een afgeleid privacyprobleem uit voortvloeit. Ik ben van mening dat deze praktijk op een ander, fundamenteler niveau bekeken moet worden.

Wanneer het om privacy of gegevensbescherminggaat, wordt vaak op concreet niveau naar een casus gekeken en per detail bepaald of iets wettelijk is toegestaan of niet. Een fundamentele benadering ontbreekt helaas vaak en dat is mede te wijten aan de formuleringen en benaderingen in de huidige regelgeving betreffende gegevensbescherming.

2 Autonomie, privacy en identiteit

Het recht op privacy is een fundamenteel recht dat geldt voor alle individuen. Van oudsher werd privacy in zekere mate gewaarborgd door natuurlijke beperkingen, zoals fysieke afstand (zeker toen er nog geen auto's en telefoons waren) en de menselijke eigenschap van 'vergeten'. Deze beperkingen zorgden ervoor dat verschillende contexten gescheiden bleven, dat de kring van mensen die ergens kennis van kon nemen beperkt was en dat dingen na verloop van tijd vergeten werden. In de huidige informatiemaatschappijzijn al deze beperkingenverdwenen. Gegevens worden digitaal opgeslagen en verwerkt, een druk op de knop zorgt dat gegevens gedeeld worden met grote groepen mensen of potentieel zelfs iedereen

---

* **Arnold Roosendaal is promovendus bij het Tilburg Institute for Law, Technology, and Society (TILT) aan Tilburg University en partner bij FennellRoosendaal Onderzoek en Advies.**

1 Zie bijvoorbeeld: C.A. Dwyer, *Behavioral Targeting: A Case Study of Consumer Tracking on Levis.com*, Paper presented at the 15th American Conference on Information Systems, San Francisco, California: 2009; D. Martin, H. Wu & A. Alsaid, *Hidden Surveillance by Web Sites: Web Bugs in Contemporary Use*, Communications of the ACM 46, no. 12ve (2003), p. 258-264.

2 Richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009 tot wijziging van Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronische communicatienetwerken en -diensten amendeert. Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie.

3 Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.

4 F.J. Zuiderveen Borgesius, 'De nieuwe cookieregels: alwetende bedrijven en onwetende internetgebruikers?', *P&I* 2011-1, p. 3-12.

5 B. van der Sloot, 'Het plaatsen van cookies ten behoeve van behavioural targeting vanuit privacyperspectief', *P&I* 2011-2, p. 62-69.

en het internet vergeet niets, er is geen 'digital oblivion', geen digitale vergetelheid. Dat betekent dat gegevens lange tijd bewaard blijven, mogelijk op verschillende plaatsen en dat een individu geen overzicht meer heeft over wie toegang heeft tot welke gegevens.

Deze karakteristieken van de informatiemaatschappij maakten het noodzakelijk om regels op te stellen voor de omgang met persoonlijke gegevens. Het recht op privacy kon immers zwaar aangetast worden wanneer gegevens over een individu in een andere context terechtkwamen dan waar ze in eerste instantie voor bedoeld waren. Ook het idee dat dingen soms vergeten moeten worden speelde een rol. In pas met deze ontwikkelingen zijn initiatievengenomen om aan de vraag naar gegevensbescherming te voldoen. De eerste grote stap was Europese Conventie 108, waarin een aantal basisprincipes voor de verwerking van persoonsgegevens zijn vastgelegd, zoals kwaliteit van gegevens en adequate beveiliging. Het aantal gegevensverwerkingen nam daarna snel toe en ook in de private sector ontstonden steeds meer databanken met persoonsgegevens. Om ook een handhavingmechanisme voor gegevensbescherming te hebben werd als vervolg op deze Conventie in 1995 de Richtlijn Gegevensbescherming geïntroduceerd. Deze Richtlijn moest door alle EU-lidstaten in nationale wetgeving worden geïmplementeerd. In de Richtlijn is onder meer duidelijk aangegeven wat legitieme gronden voor gegevensverwerking zijn. Zonder een van deze grondslagen is verwerking van persoonsgegevens niet toegestaan. Op verscheidene plaatsen in de preambule worden fundamentele rechten van het individu, in het bijzonder het recht op privacy, aangehaald als beschermenswaardig en wordt expliciet verduidelijkt dat de Richtlijn ook bedoeld is om die bescherming te bieden.

De relatie tussen gegevensbescherming en privacy is de persoonlijke levenssfeer. Op de persoonlijke levenssfeer mag niet zomaar inbreuk gemaakt worden. Maar de traditionele muren om iets binnenshuis te houden volstaan niet meer. Door het voortschrijden van de informatietechnologie kunnen dingen die in de persoonlijke levenssfeer gebeuren, steeds makkelijker in gegevens gevangen worden. Daarom dienen die gegevens dus beschermd te worden.

Privacy als bescherming van de persoonlijke levenssfeer is op haar beurt instrumenteelaan de fundamentele waarde van individuele autonomie. Die individuele autonomie houdt in dat het individu in staat is om zijn eigen keuzes te maken en zijn eigen doelen, zowel op korte als op lange termijn, te stellen. Daartoe is het noodzakelijk om vrij te kunnen beslissen en om vrij toegang te hebben tot de mogelijkhedenwaaruit gekozen kan worden. Op het moment dat anderen die keuzes of doelen al bepalen of beperken is de autonomie in het geding. Daarom is het van belang dat een individu zelf kan bepalen welke gegevens hij deelt en met wie om tot een bepaalde keuze te komen.

Het bepalen welke gegevens worden gedeeld met wie hangt weer samen met persoonlijke identiteit. Dit verband komt vooral sterk tot uitdrukking in de definitie van privacy die Rotenberg en Agre geven: Privacy is the freedom from unreasonable constraints on constructing identity and control over aspects of identity projected to the world.[6] Individuen hebben in het dagelijks leven verschillende deelidentiteiten; werknemer, golfliefhebber, ouder, etc. Bij elke identiteit horen bepaalde gegevens die gedeeld kunnen worden met anderen die tot de desbetreffende context behoren. Met je collega's op het werk bespreek je andere dingen dan met je gezin. Wanneer gegevens binnen de relevante context blijven wordt dit ook wel contextuele integriteit genoemd.[7] Die integriteit is noodzakelijk om een rol binnen een context goed te kunnen vervullen.[8] Wanneer contexten door elkaar gaan lopen kunnen keuzes beperkter worden en is uiteindelijk de autonomie aangetast.

3 Monitoring en profiling

De in de vorige paragraaf besproken concepten staan in de huidige internetpraktijk onder druk. Omdat veel communicatie via het internet geschiedt, is de computer een soort fuik geworden waar alle informatie doorheen moet. Dat betekent dat gegevens die tot verschillende contexten behoren in de computer bij elkaar komen. Op het eerste gezicht lijken de gegevens wel gescheiden te blijven, maar de realiteit is anders. Dat is te wijten aan monitoringpraktijken en cookies. Cookies zijn unieke tekstbestandjes die op de computer van internetgebruikers geplaatst worden. Aan de hand van een cookie kan een computer herkend worden, waardoor webpagina's getoond kunnen worden naargelang voorkeursinstellingen van de gebruiker. Ook kunnen aankopen uit het verleden of artikelen die bekeken zijn uitgelicht worden en op basis van eerdere aankopen aanbevelingen gedaan worden. Daarmee kan dus de gebruikerservaring verbeterd worden.[9]

Een andere belangrijke overweging voor commerciële partijen om cookies te gebruiken is het optimaliseren van inkomsten door gerichte advertenties. Hoe persoonlijker een advertentie is afgestemd, hoe groter de kans dat een internetgebruiker daadwerkelijk op de advertentie klikt. Om een advertentie goed af te stemmen is het belangrijk om te weten welke interesses een internetgebruiker heeft. Hoe gedetailleerder, hoe beter. Om die interesses te bepalen kunnen profielen gemaakt worden van individuele internetgebruikers. Cookies zijn daarbij een belangrijk hulpmiddel vanwege de mogelijkheid om internetgedrag te monitoren. Het spreekt voor zich dat een grotere hoeveelheid informatie tot een gedetailleerder profiel kan leiden. Om een grote hoeveelheid gegevens te verzamelen is het handig om een gebruiker over verschillende webpagina's te kunnen volgen. Er zijn

6 P.E. Agre & M. Rotenberg. *Technology and Privacy: The New Landscape*. Cambridge, MA [etc.]: MIT Press 1997, p. 7.
7 H. Nissenbaum, *Privacy as Contextual Integrity*, *Washington Law Review* 79 (2004): 119-58.
8 E. Goffman, *The Presentation of Self in Everyday Life*, Doubleday Anchors Books. Garden City, N.Y.: Doubleday & Company 1959.
9 Zie hierover ook het eerdergenoemde artikel van Van der Sloot.

echter enkele beperkingen aan cookies die dat technisch gezien lastiger maken.

Zoals gezegd zijn cookies kleine tekstbestandjes die door een content provider op de computer van de gebruiker worden geplaatst. Wanneer een volgende keer content van de servers van de content provider wordt opgevraagd wordt de cookie in het verzoek meegestuurd en kan de provider de computer herkennen. Een cookie wordt echter alleen meegestuurd naar de provider die de cookie geplaatst heeft. Het is mogelijk dat alle onderdelen van de server van de partij van wie de webpagina is afkomstig zijn. In dat geval is er dus alleen een interactie met de servers van de partij wiens webpagina daadwerkelijk wordt bezocht. In de praktijk zijn er echter vaak vele partijen in het spel. Een webpagina bezoeken resulteert dan in een serie contentverzoeken aan verschillende servers; ook servers van andere content providers dan de partij die je beoogt te bezoeken. Dat zijn de zogeheten third parties. De content die door deze derde partijen geleverd wordt kan bestaan uit bijvoorbeeld advertenties, plaatjes, kaarten, videomateriaal, of applicaties die onzichtbaar meedraaien en bijvoorbeeld statistieken samenstellen. Third parties kunnen content aanleveren voor verschillende webpagina's. Wanneer zij een cookie geplaatst hebben op de computer van een internetgebruiker kunnen zij deze gebruiker dus volgen over al deze pagina's, omdat de cookie meegestuurd wordt in de http-request aan de servers van deze partij, ongeacht op welke pagina de gebruiker zich bevindt.

Omdat het op het eerste gezicht niet duidelijk is dat niet alleen de beoogde webpagina wordt bezocht, maar dat er in feite met een heleboel partijen gecommuniceerd wordt, is het lastig om in te schatten welke partijen gegevens over de internetgebruiker verzamelen. Mede daarom is het lastig om toestemming voor cookiegebruik te geven middels browserinstellingen.[10] Toestemming in de zin van de Wet bescherming persoonsgegevens vereist immers geïnformeerd zijn. Doordat cookies op de achtergrond werken en de gemiddelde internetgebruiker dus vaak niet op de hoogte is van cookies en wat die doen kan er van geïnformeerd zijn geen sprake zijn. Er zijn echter ook situaties waar het lijkt of de internetgebruiker een bewuste keuze kan maken, maar waar dit juist vanwege cookies niet het geval is. Een duidelijk voorbeeld hiervan is de wijze waarop Facebook de 'Vind ik leuk'-knop[11] gebruikt.[12]

4 De 'Vind ik leuk'-knop van Facebook

De 'Vind ik leuk'-knop ('Like button') is een knop die op veel webpagina's voorkomt. Het is een 'thumbs-up'-symbool met de tekst 'Vind ik leuk' ernaast. Facebookleden kunnen op de knop klikken om aan te geven dat ze iets leuk vinden. Bij een ingelogde Facebook-gebruiker verschijnt er dan onmiddellijk een link naar het item of de betreffende webpagina op zijn of haar profielpagina. Volgens Facebook, '[t]he Like button lets a user share your content with friends on Facebook. When the user clicks the Like button on your site, a story appears in the user's friends' News Feed with a link back to your website.'[13] De code waarmee de knop geïmplementeerd kan worden in een webpagina is gratis beschikbaar en kan dus eenvoudig door website-eigenaren worden gebruikt om bezoekers de pagina of onderdelen ervan te laten promoten.

De 'Vind ik leuk'-knop is één van de zogeheten social plugins die Facebook in april 2010 op haar F8-conferentie introduceerde. De knop moest Facebook-gebruikers in staat stellen om op eenvoudige wijze interesses te delen door te verwijzen naar artikelen en pagina's. Sindsdien is de knop op tal van pagina's verschenen. De waarde van de knop is ook vanuit commercieel oogpunt aanzienlijk. Pagina's die de 'Vind ik leuk'-knop hebben geïmplementeerd, rapporteren groei in bezoekersaantallen van soms meer dan 200% en de tijd die op pagina's met de knop wordt gespendeerd om artikelen te lezen is vaak ook met 80% toegenomen.[14] De populariteit van de knop in combinatie met de enorme commerciële waarde maakt het aannemelijk dat het aantal 'Vind ik leuk'-knoppen explosief toe zal blijven nemen.

Bij het laden van de 'Vind ik leuk'-knop wordt geen cookie geplaatst. Facebook heeft daar andere methoden voor. Vanzelfsprekend krijgen leden van Facebook bij hun aanmelding een cookie met een unieke gebruikers-ID. Mensen die geen account bij Facebook hebben kunnen echter ook een cookie krijgen via Facebook Connect. Facebook Connect is een programma dat op de achtergrond van veel webpagina's draait om koppelingen tussen de pagina en Facebook mogelijk te maken, bijvoorbeeld om de link van een profielpagina naar een artikel dat iemand met de 'Vind ik leuk'-knop heeft gepromoot te maken. Wanneer Facebook Connect wordt geladen bij het bezoeken van een webpagina wordt een cookie geplaatst op de computer van de gebruiker indien deze nog geen Facebook-cookie heeft. Vanaf het moment dat de cookie er is, wordt deze elke keer meegestuurd in een http-request om content van de Facebook-servers te laden. Dat kan dus ook de 'Vind ik leuk'-knop zijn. Deze knop wordt immers geïmplementeerd in een pagina, maar is in feite een regelcode die het plaatje opvraagt van de Facebook-servers.

De 'Vind ik leuk'-knop is te vinden op een zeer grote hoeveelheid webpagina's. Facebook krijgt via al deze pagina's informatie over de bezoekers. Wat de 'Vind ik leuk'-knop bijzonder maakt ten opzichte van 'traditionele' third party cookies om internetgedrag te monitoren is de zichtbaarheid van de knop. Juist omdat de knop zichtbaar is zal een gebruiker denken zelf controle te

10 Zie hierover ook het eerdergenoemde artikel van Zuiderveen Borgesius.
11 In het Engels de 'Like button'.
12 Zie voor een uitgebreidere technische beschrijving mijn paper 'Facebook Tracks and Traces Everyone: Like This!' beschikbaar op <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1717563> en mijn bijdrage in InformatieBeveiliging: 'Facebook volgt iedere internetgebruiker: Like this!', *InformatieBeveiliging* 2011-2, p. 18-21.
13 Zie: <http://developers.facebook.com/docs/reference/plugins/like>.
14 Zie: <www.facebook.com/notes/facebook-media/value-of-a-liker/150630338305797>.

hebben over de communicatie met Facebook. Facebookleden kunnen bewust op de knop klikken om een koppeling naar hun profielpagina te maken of juist niet op de knop te klikken om dat niet te doen. De meeste mensen zullen veronderstellen dat er geen communicatie is met Facebook als ze niet op de knop klikken. Zeker internetgebruikers die (bewust) geen Facebook-lid zijn zullen ervan uitgaan dat er geen communicatie met Facebook is. Juist de zichtbaarheid van de knop en de bijbehorende functionaliteit versterken deze suggestie. Maar in werkelijkheid ziet Facebook elke bezoeker, omdat de knop van de Facebook-servers opgevraagd wordt bij het laden van een pagina. Aanklikken van de knop of lid zijn van Facebook is dus niet nodig om toch gevolgd te worden door Facebook.

Op 30 november 2010 is een artikel over deze bevindingen online gepubliceerd op SSRN.[15] Naar aanleiding hiervan is de Hamburgse privacywaakhond[16] onder leiding van prof. dr. Johannes Caspar een onderzoek gestart. In de communicatie tussen Caspar en Facebook heeft Facebook erkend dat de bevindingen juist zijn. Volgens Facebook lag het aan een programmeerfout in de software maar zou de software onmiddellijk zijn aangepast nadat zij op de hoogte waren gesteld van de onterecht gebruikte cookies en trackingmogelijkheden. Begin mei 2011 lijkt het er echter op dat de praktijk ongewijzigd is op alle sites die Connect en de 'Vind ik leuk'-knop al hadden geïmplementeerd.

5 En terug naar privacy…

Wat betekent de 'Vind ik leuk'-knop of monitoringtechnologie dan voor privacy? Zoals uit het voorgaande blijkt is er geen mogelijkheid voor internetgebruikers om toestemming te geven voor verwerking van hun gegevens of, belangrijker nog, om die toestemming te weigeren. In eerste instantie zit het probleem dus bij gegevensbescherming. Wanneer cookies worden gebruikt ten behoeve van behavioural advertising kan dat volgens Van der Sloot echter alleen een gevoel van schaamte opleveren bij het expliciteren van bepaalde voorkeuren. Daarnaast wijst hij op een 'chilling effect' wat hij feitelijk koppelt aan beveiligingsproblemen en het lekken van gegevens: gegevens komen in verkeerde handen terecht en kunnen misbruikt worden. Er is echter meer aan de hand. In hoofdlijnen kunnen aan het recht op privacy in het licht van autonomie en identiteit twee hoofdkarakteristieken worden toegeschreven: informationele zelfbeschikking en contextuele integriteit. Voornoemde problemen horen hoofdzakelijk bij informationele zelfbeschikking. Het gaat dan over de controle en zeggenschap over wie er bepaalde informatie te zien krijgt en wie bepaalde gegevens mag verwerken. Met name in het geval van datalekken is die controle verdwenen.

De tweede karakteristiek, contextuele integriteit, is echter nog niet volledig aan de orde geweest. Juist omdat internetgedrag over verschillende webpagina's gevolgd wordt raken de grenzen tussen verschillende contexten vervaagd. Bij elke context hoort echter een andere deelidentiteit. Pagina's kunnen bekeken worden voor professionele doeleinden in opdracht van een werkgever, andere pagina's worden bezocht vanuit hobbyistisch perspectief en er zijn zaken die privé dienen te blijven voor het gezin of voor de individuele gebruiker. Bij het gebruik van cookies om internetgedrag gedetailleerd in kaart te brengen gaan de contexten verloren en komen gegevens die eigenlijk gescheiden behoren te blijven bij elkaar. Eén partij heeft dus mogelijk inzicht in alle deelidentiteiten die een individu aanneemt.

Wanneer we dan kijken naar privacy als de vrijheid om een identiteit te construeren en om te controleren welke aspecten van een identiteit getoond worden[17] is al snel duidelijk dat van die vrijheid weinig sprake meer kan zijn. De identiteit, of in het geval van behavioral advertising het profiel, wordt immers door een ander geconstrueerd. Daarnaast heeft het individu geen controle over welke gegevens de basis vormen voor dat profiel en welke niet. In het specifieke geval van Facebook kunnen gegevens die verzameld worden over webgedrag gekoppeld worden aan profielpagina's van leden. Daarmee wordt het profiel dus veel uitgebreider en gedetailleerder dan de informatie die het Facebooklid bewust op zijn profielpagina heeft geplaatst. Wanneer een individu bewust kiest om voor verschillende contexten verschillende sociale netwerken te gebruiken, bijvoorbeeld Facebook voor een hobbyclub en LinkedIn voor professionele contacten, gaat die scheiding verloren, in ieder geval op het niveau van interesses.

Ook voor iemand die bewust, misschien zelfs vanuit privacyoverwegingen, geen lid van Facebook is, is de situatie alarmerend. Er kan geen koppeling aan een profielpagina gemaakt worden, maar het individu wordt wel degelijk gevolgd op het internet. Ook hier wordt een profiel gevormd door Facebook. Het verband met individuele autonomie is hier nog duidelijker aanwezig. Een bewuste keuze om geen connectie met Facebook aan te gaan is eigenlijk niet mogelijk. Daarnaast wekken de Facebook-tools juist de suggestie dat deze keuze er wel degelijk is, bijvoorbeeld door het zichtbaar tonen van de 'Vind ik leuk'-knop op webpagina's. Een voor de hand liggende verwachting is: niet klikken betekent geen contact met Facebook. Dit blijkt niet het geval te zijn.

Een laatste aandachtspunt betreft de profielen die samengesteld worden. Deze profielen kunnen erg gedetailleerd zijn en in het geval van gebruik voor behavioural advertising logischerwijs ook erg gepersonaliseerd. Het gaat dus echt om een individu en verder dan een relatief beperkte verzameling hokjes op hoofdlijnen. Daarmee is de invloed op het individu veel groter dan bij het praktische hokjesdenken (wat zelfs handig kan zijn).

Geïndividualiseerde profielen hebben ook invloed op de autonomie van individuen. Wanneer er op basis van een profiel een aantal keuzes worden aangeboden, zijn die keuzes al voorgeselecteerd. Er is dus geen overzicht

15 'Facebook Tracks and Traces Everyone: Like This!' beschikbaar op <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1717563>.
16 Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, <www.hamburg.datenschutz.de>.
17 P.E. Agre & M. Rotenberg, *Technology and Privacy: The New Landscape*, Cambridge, MA [etc.]: MIT Press 1997, p. 7.

van het complete aanbod. Het individu heeft een keuze, maar die keuze is beperkt. Dat is des te meer het geval wanneer op basis van een profiel geen keuze wordt geboden. Iets wat je niet krijgt aangeboden zie je niet. Een individu kan het dus ook niet snel missen en het is ook erg lastig om inzicht te krijgen in wat iemand allemaal niet krijgt aangeboden. Autonomie in de zin van keuzevrijheid is dus in het geding, maar ook autonomie in de zin van zelf bepalen wat je identiteit is en hoe je als individu jezelf wilt presenteren staat onder druk.

De sterke individualisatie van profielen betekent dat het echt om een individu gaat, ongeacht of de naam van dat individu bekend is bij degene die het profiel beheert. Het vasthouden aan argumenten dat de wet niet van toepassing zou zijn, omdat het anonieme gegevens zouden zijn, is daarom echt niet langer houdbaar. De uitdaging is om alternatieven te vinden.

6 Een blik in de toekomst

Het vinden van alternatieven om gegevens en uiteindelijk privacy en autonomie goed te beschermen is niet eenvoudig. Wel kunnen uit de huidige technologische praktijk concrete aandachtspunten worden gedestilleerd die een aanzet geven tot een denkrichting. Naar mijn mening zijn twee punten essentieel. Het eerste is dat het onderscheid tussen persoonsgegevens en andere gegevens niet relevant meer is. Het tweede punt is dat het tegenwoordig hoofdzakelijk gaat om grote gegevenssets in plaats van kleine sets van losse gegevens.

Met betrekking tot het eerste punt is recent een belangrijke stap gezet in de Verenigde Staten. De Federal Trade Commission (FTC) heeft in december 2010 een stafrapport uitgebracht over consumentenbescherming in een tijdperk van snelle veranderingen.[18] Een van de belangrijkste punten in dat rapport is dat het onderscheid tussen PII[19] en PI (Personal Information) niet meer relevant is. Dit is overigens een punt dat in Europa al veel langer onderkend is. Ook zonder de naam, adres en woonplaats te kennen, kunnen individuen bereikt worden en persoonlijk benaderd op basis van profielen. Dat gebeurt dan via een computer of ander apparaat waarmee digitale interactie (hoofdzakelijk internet) plaats kan vinden. Vanzelfsprekend kunnen deze apparaten door meerdere personen gebruikt worden. Echter, veel apparaten worden persoonlijk vanwege de mobiliteit, zoals laptops en smartphones. Daarnaast is de technologie al ver genoeg om aan de hand van surfgedrag verschillende gebruikers te onderscheiden. In zijn rapport stelt de FTC een aantal maatregelen voor om privacy van consumenten en veiligheid van gegevens beter te waarborgen. De FTC stelt daarbij een nieuwe definitie voor van het begrip consumentengegevens.[20] Het voorgestelde raamwerk zou van toepassing moeten zijn op: 'all commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or other device.'[21] Wanneer er dus een mogelijkheid is om een specifieke consument óf computer of ander apparaat te koppelen aan gegevens zijn de maatregelen van toepassing. Hierin is de verschuiving van personen naar devices en daarmee ook van PII naar 'personal information' treffend vastgelegd. Het is belangrijk dat de FTC deze verschuiving expliciet maakt, omdat veel grote internetbedrijven zoals Facebook en Google hun thuisbasis in de Verenigde Staten hebben en dus in de eerste plaats aan Amerikaanse regelgeving gebonden zijn. De controle op dergelijke bedrijven kan daardoor wellicht aangescherpt worden.

Als specifieke maatregelen zet de FTC sterk in op 'privacy by design', waarbij bedrijven privacybescherming in hun dagelijkse gang van zaken in moeten bouwen. Consumenten moeten daarnaast eenvoudiger keuzes kunnen maken over wat er met hun gegevens gebeurt. De controle door het individu wordt belangrijk gevonden en moet ook praktisch uitvoerbaar zijn. Eén van de manieren om dat te bereiken is een zogenoemd 'Do Not Track'-systeem, bijvoorbeeld in de vorm van een instelling in de browser die de voorkeuren van de gebruiker doorgeeft voor wat betreft tracking en het ontvangen van targeted advertisements.[22] Naast deze drie hoofdpunten geeft de FTC aan dat ze de toegang voor consumenten tot hun gegevens wil verbeteren en ook wil werken aan bewustwording door educatieve maatregelen.

In Europa is de herziening van de Privacyrichtlijn in volle gang. Controle en transparantie horen bij de basisprincipes die ten grondslag liggen aan de Richtlijn en worden sterk benadrukt als uitgangspunten bij de herziening. De Artikel 29-Werkgroep noemt bijvoorbeeld toestemming en transparantie als aandachtspunten voor verduidelijking, maar ook nieuw toe te voegen principes, zoals privacy by design en accountability.[23] Het tweede punt is echter nog niet afgedekt en dat lijkt ook een stuk lastiger. Traditioneel wordt er gekeken of een gegeven kwalificeert als persoonsgegeven in de zin van de Wet bescherming persoonsgegevens. Is dat het geval, dan is de wet van toepassing. Voor kwalificatie als persoonsgegeven is directe of indirecte herleidbaarheid naar een natuurlijk persoon vereist. Bij directe herleidbaarheid treden doorgaans weinig problemen op, maar indirecte herleidbaarheid is vaak lastiger. Dit heeft mede te maken met het feit dat gegevens voor een verwerker niet her-

18 Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change*. Online beschikbaar: <www.ftc.gov/os/2010/12/101201privacyreport.pdf>.

19 Personally Identifiable Information, de Amerikaanse vorm van persoonsgegevens, die overigens veel beperkter is dan bij ons, omdat het alleen gaat om een combinatie van social security number, naam en meer.

20 In de VS is privacy alleen in specifieke sectoren wettelijk beschermd. Er is een grote rol weggelegd voor consumentenbescherming tegen oneerlijke en misleidende handelspraktijken.

21 Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change*, p. 42.

22 Een concrete uitwerking van dit voorstel wordt gegeven in een reactie van Stanford University op het rapport: J. Mayer & A. Narayanan, *Re: Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, 18 februari 2011. Online beschikbaar: <http://donottrack.us/docs/FTC_Privacy_Comment_Stanford.pdf>.

23 Artikel 29-Werkgroep, *The Future of Privacy*, WP 168 van 1 december 2009. Online beschikbaar: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf>.

leidbaar kunnen zijn, maar wel voor een andere partij die toegang tot de gegevens krijgt.

Een vorm van indirecte herleidbaarheid is wanneer een koppeling aan andere gegevens mogelijk is waardoor een gegeven te herleiden is naar een natuurlijk persoon. In zekere zin wordt er dus ook iets gezegd over gegevenssets of over gekoppelde gegevens. Tegenwoordig gaat het echter hoofdzakelijk om gegevenssets en is het erg gekunsteld om een discussie te voeren over of een totale set al dan niet herleidbaar is tot een natuurlijk persoon wanneer er geen naam of ander direct identificerend gegeven beschikbaar is. Het zou daarom beter aansluiten om van de complete sets gegevens uit te gaan en te kijken of aan de hand daarvan een individu *bereikt* kan worden. De nadruk komt dan meer te liggen op de gegevensset als totaalplaatje dat een individu digitaal representeert. Hoe dit wettelijk vastgelegd zou kunnen worden en in wat voor vorm is echter op dit moment lastig te zeggen.

7 Conclusie

Ondanks dat er op dit moment geen sluitend alternatief voorhanden is, is het goed om te zien dat erkend wordt dat de technologie de wijze van communiceren en de manier waarop individuen benaderd worden, sterk heeft veranderd. Wanneer privacy en autonomie goed beschermd dienen te blijven, onder andere door gegevensbescherming en vrije identiteitsvorming, is het noodzakelijk om nieuwe benaderingen te zoeken ten aanzien van gegevenssets. Individuen worden wel degelijk geraakt in hun privacy en autonomie als gevolg van monitoring en profilingtechnologiën. De uitdaging ligt in het vinden van alternatieve oplossingen, maar in ieder geval heeft de FTC al een stap in de goede richting gezet. Ook de EU zou bij de herziening van de Dataprotectierichtlijn sterk rekening moeten houden met het bestaan van gegevenssets, de toenemende onmogelijkheid van anonimisering dan wel de toenemende mogelijkheid van identificatie door derden, en dat herleidbaarheid tot een persoon ook vaak mogelijk is op machineniveau. Een naam is niet nodig. Het herkennen van een computer en mogelijk vaststellen dat een bepaalde gebruiker achter die computer zit is voldoende.